RESPONSE   Serial No. 09/859,667
Examiner: JUNG, David Yiuk   Atty. Docket No.: 42336.010500

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A system for at least one secure networking ~~data transmission~~ session between a requestor and a resource comprising:

a secure point of presence, wherein a networking protocol is implemented on the secure point of presence, and wherein the secure point of presence facilitates the creation of the at least one secure networking session between the requestor making a request and the resource;

a session layer, implemented within the networking protocol, wherein the session layer ~~that~~ maps authentication of the at least one secure networking session associated with at least one request to authorization information associated with the secure networking session ~~level authorization~~, wherein the authorization information associated with the secure networking session level ~~authorization defining~~ defines permitted communications between the at least one resource and the at least one requestor for the at least one secure networking session.

2. (Currently Amended) The system of claim 1, wherein the session layer further comprises ~~includes~~:

a trusted session sub-layer, wherein the trusted session sub-layer is implemented as part of the session layer, for networking session level authorization and maintenance; and,

a reverse proxy for transferring data between the at least one resource and the at least one request.

3. (Currently Amended) The system of claim 2, wherein the network protocol stack layers ~~of the request~~ below ~~its~~ the trusted session sub-layer associated with the request are unaware of existence of network protocol layers associated with ~~of~~ the resource below ~~it's~~ the trusted session sub-layer.

4. (Original) The system of claim 1, wherein the session layer forms a bundle of transport layer connections between the at least one resource and the at least one request.

- 2 -

5. (Original) The system of claim 4, wherein a plurality of bundles of transport layer connections are joined to create a meta-session.

6. (Original) The system of claim 1, wherein the session layer maps ports onto itself.

7. (Original) The system of claim 6, wherein the session layer associates a transport connection for data to pass from the at least one resource to the at least one request.

8. (Original) The system of claim 1, further including a trusted operating system.

9. (Original) The system of claim 1, wherein the authorizations are dynamically updated.

10. (Original) The system of claim 1, wherein no layer below the session layer communicates on a peer to peer level.

11. (Original) The system of claim 1, wherein the session layer includes a sterile core.

12. (Original) The system of claim 1, wherein the session layer maps the authentication of users using a Secure Core rulebase.

13. (Original) The system of claim 1, wherein resource identities are masked.

14. (Original) The system of claim 1, wherein the authorization is dependent on a network interface of the at least one request.

15. (Original) The system of claim 1, wherein the session layer provides an audit trail.

16. (Currently Amended) The system of claim 1, wherein the session layer can establish multiple bi-directional sessions with multiple requests, each session operating in a half-duplex manner.

17. (Original) The system of claim 1, wherein the session layer mediates resources between the at least one request and the at least one resource based on a credential set.

18. (Original) The system of claim 1, wherein the session layer mediates resources between the at least one request and the at least one resource based on a credential set, and wherein the session layer bundles transport layer communications between the at least one resource and the at least one request by associating the bundles with the credential set.

19. (Original) The system of claim 1, further including a multi-level operating system used as a proxy.

- 3 -

20. (Original) The system of claim 1, further including a Session Manager to communicate through higher OSI layers.

21. (Original) The system of claim 1, wherein no physical resource is time-division shared by the at least one resource requester and the at least one resource provider.

22. (Currently Amended) A system for <u>implementing a</u> secure <u>networking</u> data transmission <u>session between a user and a resource provider,</u> comprising:

a virtual air gap ~~provided by:~~ <u>comprising</u> a trusted session sub-layer <u>wherein the trusted sub-layer is implemented within a session layer of a network protocol stack, wherein the trusted sub-layer performs networking data transmission</u> ~~-for~~ session authorization and maintenance, <u>and wherein the virtual air gap separates requests received from the user from resources provided by the resource provider;</u>

<u>a reverse proxy for data transfer between a user and a resource provider; and,</u>

a trusted operating system for <u>networking data transmission</u> session separation, <u>wherein the trusted operating system runs the reverse proxy, and wherein the virtual air gap is implemented as part of the trusted operating system.</u>~~; and,~~

~~a reverse proxy for data transfer between a user and a resource provider.~~

23. (Currently Amended) The system of claim 22, wherein ~~of~~ the <u>network protocol stack layers associated with the</u> user <u>request</u> ~~layers~~ below <u>the</u> ~~its~~ trusted session sub-layer are unaware of existence of <u>network protocol stack</u> layers <u>associated with</u> ~~of~~ the resource provider below ~~its~~ <u>the</u> trusted session sub-layer.

24. (Original) The system of claim 22, wherein the trusted session sub-layer forms a bundle of transport layer connections between the user and the resource provider.

25. (Original) The system of claim 24, wherein a plurality of bundles of transport layer connections are joined to create a meta-session.

26. (Currently Amended) The system of claim 22, wherein <u>the</u> ~~a~~ session layer~~, which includes the trusted session sub-layer,~~ <u>is capable of mapping</u> ~~maps~~ ports onto itself.

27. (Original) The system of claim 22, wherein the session authorization is dynamically updated.

- 4 -

RESPONSE   Serial No. 09/859,667
Examiner: JUNG, David Yiuk   Atty. Docket No.: 42336.010500

28. (Currently Amended) The system of claim 22, wherein ~~no~~ <u>network protocol stack</u> layers below <u>the</u> ~~a~~ session layer, ~~which includes the trusted session sub-layer,~~ <u>do not</u> communicates on a peer to peer level.

29. (Original) The system of claim 22, wherein the trusted session sub-layer maps user authentication using a Secure Core rulebase.

30. (Currently Amended) The system of claim 22, wherein the <u>networking data transmission</u> session authorization is dependent on <u>a</u> network interface <u>type used by</u> ~~of~~ the user.

31. (Original) The system of claim 22, wherein the trusted session sub-layer mediates resources between the user and the resource provider based on a credential set.

32. (Original) The system of claim 22, wherein the trusted session sub-layer mediates resources between the user and the resource provider based on a credential set, and wherein the trusted session sub-layer bundles transport layer communications between the user and the resource provider by associating the bundles with the credential set.

33. (Original) The system of claim 22, further including a multi-level operating system used as a proxy.

34. (Original) The system of claim 22, further including a Session Manager to communicate through higher OSI layers.

35. (Original) The system of claim 22, wherein no physical resource is time-division shared by the user and the resource provider.

36. (Currently Amended) A system for secure <u>networking</u> data transmission <u>utilizing a networking protocol stack, the system</u> comprising:

a trusted session sub-layer<u>, wherein the trusted session sub-layer is implemented within a session layer of the networking protocol stack, and wherein the trusted session sub-layer maintains</u> ~~maintaining~~ a virtual air gap between a plurality of resource requesters and a plurality of resource providers; <u>and,</u>

a session manager<u>, wherein the session manager controls data transfers</u> ~~for a transfer of data~~ between the plurality of resource requesters and the plurality of resource providers.

- 5 -

37. (Original) The system of claim 36, wherein the trusted session sub-layer includes a reverse proxy for transferring data between the plurality of resource requesters and the plurality of resource providers.

38. (Original) The system of claim 36, wherein the trusted session sub-layer forms a bundle of transport layer connections between the plurality of resource requesters and the plurality of resource providers.

39. (Original) The system of claim 38, wherein a plurality of bundles of transport layer connections are joined to create a meta-session.

40. (Original) The system of claim 36, wherein the trusted session sub-layer maps ports onto itself.

41. (Original) The system of claim 40, wherein the trusted session sub-layer associates transport connections for data to pass from the plurality of resource requesters to the plurality of resource providers.

42. (Original) The system of claim 36, wherein authorizations for the plurality of resource requesters are dynamically updated.

43. (Currently Amended) The system of claim 36, wherein no <u>networking protocol stack</u> layer below <u>the</u> a session layer, which includes the trusted session sub-layer, communicates on a peer to peer level.

44. (Currently Amended) The system of claim 36, wherein the session layer mediates resources between the plurality of resource requesters and the plurality of resource providers based on <u>a credential set associated with</u> each resource <u>requester</u> requester's credential set, and wherein the session layer bundles transport layer communications between the plurality of resource requesters and the plurality of resource providers by associating the bundles with the <u>credential set associated with</u> each resource <u>requester.</u> requester's credential set.

45. (Original) The system of claim 36, wherein no physical resource is time-division shared by the plurality of resource requesters and the plurality of resource providers.

46. (Currently Amended) A system for secure <u>networking</u> data transmission comprising <u>a</u> <u>networking protocol stack, the networking protocol stack comprising</u>:

- 6 -

RESPONSE
Examiner: JUNG, David Yiuk

Serial No. 09/859,667
Atty. Docket No.: 42336.010500

a rulebase for authenticating authorization of the plurality of resource requesters on a
dynamic basis; and

a trusted session sub-layer, wherein the trusted session sub-layer facilitates for peer-to-peer
communication between a plurality of resource requesters and a plurality of resource
providers, wherein the trusted session sub-layer is implemented within the session layer
of the networking protocol stack, and a rulebase for authenticating authorization of the
plurality of resource requesters on a dynamic basis, wherein the trusted session sub-layer
forms a bundle of transport layer connections between the plurality of resource providers
and the plurality of resource requesters.

47. (Original) The system of claim 46, wherein the trusted session sub-layer includes a reverse
proxy for transferring data between the plurality of resource requesters and the plurality of
resource providers.

48. (Currently Amended) The system of claim 46, wherein instances of the networking protocol
stack layers can be associated with a resource requestor or a resource provider, and wherein
networking protocol stack layers of each resource requester below its the trusted session
sub-layer associated with each resource requester are unaware of the existence of
networking protocol stack layers associated with of each resource provider below the its
trusted session sub-layer.

49. (Original) The system of claim 46, wherein the trusted session sub-layer maps ports onto
itself.

50. (Original) The system of claim 46, wherein the authorizations for each resource requester are
dynamically updated.

51. (Original) The system of claim 46, wherein no layer below the session layer communicates
on a peer to peer level.

52. (Original) The system of claim 46, wherein the session layer mediates resources between the
plurality of resource requesters and the plurality of resource providers based on each user's
credential set, and wherein the session layer bundles transport layer communications
between the plurality of resource requesters and the plurality of resource providers by
associating the bundles with the each user's credential set.

53. (Currently Amended) A system for secure <u>networking</u> data transmission comprising <u>a</u>
<u>networking protocol stack, the networking protocol stack comprising</u>:

  a session layer<u>, wherein the session layer facilitates</u> ~~for a~~ <u>data</u> transfer ~~of data~~ between a
  plurality of resource requesters and a plurality of resource providers, <u>and</u> wherein <u>the</u>
  <u>networking protocol stack prohibits</u> ~~no~~ peer-to-peer connections ~~exist~~ below the session
  layer; and

  a trusted session sub-layer<u>, wherein the trusted session sub-layer operates within the session</u>
  <u>layer and maintains</u> ~~maintaining~~ a virtual air gap, <u>and</u> wherein <u>the virtual air gap is</u>
  <u>implemented such that</u> no physical resources are time-division shared between any
  resource provider and any resource requester.

54. (Currently Amended) A system for secure <u>networking</u> data transmission <u>within a networking</u>
<u>session</u> comprising <u>a networking protocol stack, the networking protocol stack comprising</u>:

  <u>a</u> session layer<u>, wherein the session layer maps</u> ~~means for mapping~~ authentication of at least
  one request to <u>networking</u> session level authorization, <u>and wherein</u> the authorization
  <u>defines</u> ~~defining~~ permitted communications between at least one resource and the at least
  one request.

55. (Currently Amended) A system for secure <u>networking</u> data transmission<u>, wherein the</u>
<u>networking data transmission comprises a plurality of networking sessions, the system</u>
comprising <u>a networking protocol stack, the networking protocol stack comprising</u>:

  <u>a</u> virtual air gap<u>, wherein the virtual air gap is</u> ~~means~~ provided ~~by:~~ <u>by a</u> trusted session sub-
  layer<u>, wherein the trusted session sub-layer is implemented as a sub-layer of the session</u>
  <u>layer of the networking protocol stack, and wherein the trusted session sub-layer</u>
  <u>performs networking</u> ~~means for~~ session authorization and maintenance;

  a trusted operating system for <u>implementing separation of the plurality of networking</u>
  <u>sessions</u> ~~session separation~~; and,

  <u>a</u> reverse proxy<u>, wherein the reverse proxy facilitates</u> ~~means for~~ data transfer between a user
  and a resource provider.

56. (Currently Amended) A system for secure <u>networking</u> data transmission comprising <u>a</u>
<u>networking protocol stack, the networking protocol stack comprising</u>:

a trusted session sub-layer, wherein the trusted session sub-layer is implemented within the

session layer of the networking protocol stack, and wherein the trusted session sub-layer

maintains ~~means maintaining~~ a virtual air gap between a plurality of resource requesters

and a plurality of resource providers; and,

a session manager, wherein the session manager manages ~~means for~~ transferring data

between the plurality of resource requesters and the plurality of resource providers.

57. (Currently Amended) A system for secure networking data transmission comprising a
networking protocol stack, the networking protocol stack comprising:

a rulebase for authenticating authorization of the plurality of resource requesters on a
dynamic basis; and

a trusted session sub-layer, wherein the trusted session sub-layer is implemented within the

session layer of the networking protocol stack, wherein the trusted session sub-layer

facilitates ~~means for~~ peer-to-peer communication between a plurality of resource

requesters and a plurality of resource providers, and ~~; a rulebase for authenticating~~

~~authorization of the plurality of resource requesters on a dynamic basis,~~ wherein the

trusted session sub-layer ~~means~~ forms a bundle of networking protocol stack transport

layer connections between the plurality of resource providers and the plurality of resource

requesters.

58. (Currently Amended) A system for secure networking data transmission comprising a
networking protocol stack, the networking protocol stack comprising:

a session layer, wherein the session layer facilitates ~~means for a transfer of~~ data transfer

between a plurality of resource requesters and a plurality of resource providers, and

wherein the session layer comprises a trusted session sub-layer, wherein the trusted

session sub-layer maintains a virtual air gap, and wherein the virtual air gap is configured

such that physical resources are not time-division shared between any resource provider

and any resource requester;

- 9 -

RESPONSE   Serial No. 09/859,667
Examiner: JUNG, David Yiuk   Atty. Docket No.: 42336.010500

wherein the networking protocol stack prevents ~~no~~ peer-to-peer connections from existing below the session layer ~~means; and trusted session sub-layer means maintaining a virtual air gap, wherein no physical resources are time-division shared between any resource provider and any resource requester.~~

59. (Currently Amended) A computer program product for secure networking data transmission, the computer program product implementing a networking protocol stack, the networking protocol stack comprising:

a computer usable medium having computer readable program code ~~means~~ embodied in the computer usable medium, wherein the computer readable program code causes ~~for causing~~ an application program to execute on a computer system, the computer readable program code ~~means~~ comprising: computer readable program networking session layer code, wherein the networking session layer code facilitates ~~means for~~ mapping authentication of at least one request to networking session level authorization, wherein the networking session level authorization defines ~~defining~~ permitted communications between at least one resource and the at least one request.

60. (Currently Amended) A computer program product for secure networking data transmission among a plurality of networking sessions, the computer program product implementing a networking protocol stack, the networking protocol stack comprising:

a computer usable medium having computer readable program code ~~means~~ embodied in the computer usable medium, wherein the computer readable program code causes ~~for causing~~ an application program to execute on a computer system, the computer readable program code implementing a trusted session sub-layer, wherein the trusted session sub-layer facilitates network session authorization and maintenance, whereby the trusted session sub-layer creates a virtual air gap;~~means comprising: computer readable program code means for a virtual air gap provided by: computer readable program code trusted session sub-layer means for session authorization and maintenance;~~

a trusted operating system for networking session separation; and,

computer readable program code implementing a reverse proxy, wherein the reverse proxy coordinates ~~means for~~ data transfer between a user and a resource provider.

- 10 -

61. (Currently Amended) A computer program product for secure <u>networking</u> data transmission, <u>the computer program product implementing a networking protocol stack, the networking protocol stack</u> comprising:

a computer usable medium having computer readable program code ~~means~~ embodied therein, <u>wherein the computer readable program code causes</u> ~~in the computer usable medium for causing~~ an application program to execute on a computer system, the computer readable program code ~~means~~ comprising:~~-~~computer readable program code <u>implementing a</u> trusted session sub-layer <u>within a session layer of the networking protocol stack, wherein the trusted session sub-layer maintains</u> ~~means for maintaining~~ a virtual air gap between a plurality of resource requesters and a plurality of resource providers; <u>and,</u>

computer readable program code <u>implementing a</u> session manager, <u>wherein the session manager transfers</u> ~~means for transferring~~ data between the plurality of resource requesters and the plurality of resource providers.

62. (Currently Amended) A computer program product for secure <u>networking</u> data transmission, <u>the computer program product implementing a networking protocol stack, the networking protocol stack</u> comprising:

a computer usable medium having computer readable program code ~~means~~ embodied therein, <u>wherein the computer readable program code causes</u> ~~in the computer usable medium for causing~~ an application program to execute on a computer system, <u>wherein</u> the computer readable program code <u>comprises</u> ~~means comprising:~~computer readable program code <u>implementing a</u> trusted session sub-layer ~~means~~ <u>as part of a session layer of the networking protocol stack, wherein the trusted session sub-layer facilitates</u> ~~for~~ peer-to-peer communication between a plurality of resource requesters and a plurality of resource providers, <u>wherein the trusted session sub-layer is capable of forming a bundle of transport layer connections between the plurality of resource providers and the plurality of resource requesters; and,</u>

- 11 -

a rulebase for authenticating authorization of the plurality of resource requesters on a

dynamic basis.~~, wherein the trusted session sub-layer means forms a bundle of transport~~

~~layer connections between the plurality of resource providers and the plurality of resource~~

~~requesters~~.

63. (Currently Amended) A computer program product for secure <u>networking</u> data transmission,
<u>the computer program product implementing a networking protocol stack, the networking</u>
<u>protocol stack</u> comprising:

a computer usable medium having computer readable program code ~~means~~ embodied
<u>therein, wherein the computer readable program code causes</u> ~~in the computer usable~~
~~medium for causing~~ an application program to execute on a computer system, the
computer readable program code <u>comprises</u> ~~means comprising:~~ computer readable
program code <u>implementing a networking protocol stack</u> session layer<u>, wherein the</u>
<u>networking protocol stack session layer transfers</u> ~~means for transferring~~ data between a
plurality of resource requesters and a plurality of resource providers, wherein <u>the</u>
<u>networking protocol stack is implemented such that</u> ~~no~~ peer-to-peer connections ~~exist~~ <u>are</u>
<u>not permitted</u> below ~~the computer readable program code~~ <u>networking protocol stack</u>
session layer ~~means~~; and<u>,</u>

computer readable program code <u>implementing a</u> trusted session sub-layer<u>, wherein the</u>
<u>trusted session sub-layer is implemented within the networking protocol stack session</u>
<u>layer, and wherein the trusted session sub-layer maintains</u> ~~means for maintaining~~ a virtual
air gap, <u>wherein the virtual air gap is configured such that</u> ~~wherein no~~ physical resources
are <u>not</u> time-division shared between any resource provider and any resource requester.

64. (Currently Amended) A method for secure <u>networking</u> data transmission comprising:

<u>initiating a networking session; and,</u>

mapping authentication of at least one request to <u>networking</u> session level authorization in a
<u>networking protocol stack</u> session layer, the authorization defining permitted
communications between at least one resource and the at least one request<u>within the</u>
<u>networking session.</u>

- 12 -